Observatoire ARGA

ARGA Atlas

СТЕЙБЛКОИНЫ, САНКЦИОННЫЙ КОМПЛАЕНС И ЗАЩИТА АКТИВОВ: НОВЫЕ РИСКИ ДЛЯ ВЛАДЕЛЬЦЕВ ЦИФРОВЫХ АКТИВОВ

Авторы:

Сергей Храбрых — президент ARGA, PhD,

Наталия Цмакалова

Организация: Observatoire ARGA, ARGA Atlas

Адрес для корреспонденции: 21 route de l'Aviation, 12 C, 64600 Anglet, FRANCE

Контакты: info@argaobservatory.org, +33 7 58 49 62 27

Сайт: www.argaobservatory.org, https://www.arga-atlas.com/

Англет, 7 мая 2026

Цель документа

Настоящий доклад подготовлен с целью комплексного анализа правовых и практических рисков, возникающих при использовании стейблкоинов и иных цифровых активов в условиях усиливающегося санкционного регулирования, комплаенс-контроля и международного обмена информацией. Особое внимание уделяется тому, каким образом решения эмитентов стейблкоинов, криптовалютных платформ, поставщиков кастодиальных услуг и государственных органов могут приводить к блокировке активов, ограничению доступа к средствам и существенным имущественным потерям.

Практическая задача документа состоит в выявлении ситуаций, в которых цифровые активы, традиционно воспринимаемые как инструмент технологической автономии и трансграничной мобильности капитала, становятся объектом централизованного контроля, санкционного давления, внутренней оценки риска и правовой неопределённости. Доклад также направлен на разработку модели защиты владельцев активов в случаях блокировки кошельков, замораживания токенов, прекращения обслуживания и отказа в восстановлении доступа.

Для ARGA данная тема имеет стратегическое значение, поскольку всё больше клиентов, предпринимателей, инвесторов и лиц, находящихся в трансграничных спорах, используют стейблкоины и криптовалютные платформы как альтернативу традиционной банковской инфраструктуре. Однако на практике эти инструменты также подвержены решениям частных компаний, требованиям санкционного законодательства и механизмам международного комплаенса, способным привести к немедленному ограничению доступа к активам.

Настоящий доклад рассматривает стейблкоины и связанные с ними правовые риски как часть более широкой системы защиты собственности, цифровых прав, международного финансового регулирования и прав человека. Его задача состоит в формировании практического подхода, пригодного для адвокатов, владельцев активов, финансовых консультантов, комплаенс-специалистов и международных правозащитных механизмов.

ОГЛАВЛЕНИЕ

Executive Summary

Стейблкоины заняли центральное место в современной инфраструктуре цифровых активов. Их ключевая функция состоит в обеспечении относительной ценовой стабильности и возможности быстро перемещать стоимость между юрисдикциями, биржами, кошельками и пользователями без обращения к традиционной банковской системе. Наиболее распространённые стейблкоины используются для расчётов, хранения ликвидности, трансграничных переводов, защиты капитала и доступа к глобальным финансовым рынкам.

Одновременно развитие этого сегмента привело к появлению новых форм юридической зависимости. В отличие от классических криптовалют, многие стейблкоины выпускаются централизованными эмитентами, которые обладают технической возможностью замораживать токены, блокировать адреса, выполнять требования регуляторов и применять собственные правила оценки риска. Пользователь может считать, что владеет полностью контролируемым цифровым активом, однако фактически его доступ к средствам зависит от решений частной компании и международной комплаенс-инфраструктуры.

В условиях санкционного регулирования, усиления требований по противодействию легализации преступных доходов, роста роли аналитики блокчейна и развития таких нормативных режимов, как MiCA, использование стейблкоинов становится не только технологическим, но и правовым вопросом. Ошибочная идентификация адреса, ассоциация с высокорискованной юрисдикцией, участие в спорной транзакции или связь с лицом, находящимся под расследованием, могут привести к блокировке активов без предварительного судебного решения.

Центральный вывод настоящего доклада заключается в том, что владельцы цифровых активов должны рассматривать стейблкоины не как полностью автономный инструмент, а как часть регулируемой финансовой среды, где права собственности, доступ к активам и возможность совершения операций зависят от сочетания технологий, контрактных условий, санкционных правил, внутренней оценки риска и международных правовых стандартов.

Context & Problem Statement / Почему эта тема имеет правовое и международное значение

Стейблкоины стали одним из наиболее востребованных инструментов глобальной цифровой экономики. Они используются для хранения ликвидности, международных расчётов, перевода средств между юрисдикциями, торговли на криптовалютных рынках, расчётов с подрядчиками, сохранения стоимости в условиях валютных ограничений и быстрого доступа к цифровой финансовой инфраструктуре. Для многих пользователей стейблкоины воспринимаются как технологическая альтернатива банковскому счёту, особенно в ситуациях, когда традиционные финансовые каналы ограничены, нестабильны или недоступны.

Однако такая модель создает особую правовую иллюзию. Пользователь видит актив на собственном кошельке и полагает, что полностью контролирует средства. На практике же значительная часть популярных стейблкоинов выпускается централизованными эмитентами, обладающими возможностью технического замораживания токенов, блокировки конкретных адресов и исполнения предписаний регуляторов и правоохранительных органов. Формально токены находятся у пользователя, но фактическая возможность распоряжения ими зависит от решений третьих лиц. Соответственно, практический контроль над цифровыми активами может оставаться зависимым от централизованных технических и договорных ограничений.

Особую роль играют санкционные режимы, требования по противодействию легализации преступных доходов и внутренние комплаенс-процедуры эмитентов и платформ. Современные инструменты анализа блокчейна позволяют отслеживать происхождение активов, устанавливать связи между адресами и присваивать кошелькам определённые

категории риска. Даже если владелец актива не совершал противоправных действий, техническая связь с адресом, ранее использованным третьими лицами, может привести к ограничениям.

Значение данной темы выходит далеко за рамки криптовалютной индустрии. Стейблкоины используются предпринимателями, инвесторами, мигрантами, участниками трансграничных споров и лицами, которым требуется быстрый доступ к ликвидности вне традиционной банковской системы. Их блокировка может повлечь невозможность оплачивать юридическую защиту, выполнять договорные обязательства, финансировать бизнес, обеспечивать повседневные расходы и сохранять доступ к капиталу.

Для ARGA тема имеет стратегическое значение, поскольку всё больше трансграничных дел затрагивает цифровые активы как элемент структуры собственности и финансовой мобильности. В таких ситуациях правовая защита должна учитывать не только вопросы владения токенами, но и полномочия эмитентов, юрисдикционные риски, санкционное регулирование, комплаенс-практику и международные стандарты защиты права собственности.

Legal Framework / Нормативная и институциональная рамка

Нормативная база, регулирующая использование стейблкоинов и иных цифровых активов, представляет собой быстро развивающуюся и многоуровневую систему, в которой сочетаются частноправовые договорные условия, национальное законодательство, международные стандарты финансового мониторинга, санкционные режимы и наднациональное регулирование. Для владельца цифровых активов это означает, что техническое владение токеном неразрывно связано с юридическими механизмами, способными ограничить или полностью заблокировать доступ к средствам.

Первый уровень регулирования составляют условия выпуска и обращения конкретного стейблкоина. Эмитенты закрепляют в пользовательских соглашениях и внутренних политиках право замораживать токены, ограничивать операции, блокировать адреса и выполнять требования судов, регуляторов и правоохранительных органов. Эти документы фактически определяют объём реального контроля пользователя над активом.

Второй уровень включает национальное гражданское, финансовое и уголовное законодательство, регулирующее права собственности, обязательственные отношения, меры по аресту имущества, изъятию активов и исполнению судебных решений. Во многих юрисдикциях цифровые активы уже рассматриваются как имущество, которое может быть предметом ареста, взыскания и иных ограничений.

Третий уровень образуют нормы о противодействии легализации преступных доходов и финансированию терроризма. Банки, криптовалютные биржи, кастодиальные сервисы и эмитенты обязаны применять риск-ориентированный подход, проводить идентификацию клиентов, анализировать происхождение средств и реагировать на признаки подозрительной активности.

Четвёртый уровень составляют международные санкционные режимы, прежде всего ограничения, вводимые Office of Foreign Assets Control, Советом Европейского союза, United Nations Security Council и иными компетентными органами. Эти меры могут запрещать проведение операций, блокировать активы и обязывать частные компании прекращать обслуживание определённых лиц, адресов или категорий транзакций.

Пятый уровень формируют международные стандарты Financial Action Task Force, включая рекомендации по виртуальным активам, поставщикам услуг, идентификации клиентов, передаче информации о переводах и управлению рисками.

Шестой уровень включает наднациональное регулирование, в частности European Union. Особое значение имеет Регламент MiCA, устанавливающий требования к эмитентам и поставщикам услуг, правила раскрытия информации, корпоративного управления и защиты пользователей. Дополнительную роль играют положения о переводах криптоактивов и обязательной передаче данных о плательщике и получателе.

Седьмой уровень образуют внутренние процедуры криптовалютных бирж, аналитических компаний, поставщиков кастодиальных услуг и эмитентов стейблкоинов. Именно эти организации часто принимают наиболее значимые решения: блокируют адреса, замораживают токены, ограничивают вывод средств и требуют дополнительные документы. С технической точки зрения это может происходить почти мгновенно; с юридической точки зрения пользователь сталкивается с частным решением, имеющим последствия, сопоставимые с государственным ограничением.

Восьмой уровень связан с судебной практикой и международными стандартами защиты собственности. Национальные суды, European Court of Human Rights и другие международные органы всё чаще рассматривают цифровые активы как объект имущественных прав, а значит ограничения в отношении таких активов должны соответствовать требованиям законности, необходимости, процессуальной справедливости и соразмерности.

Таким образом, использование стейблкоинов находится на пересечении технологий, частных договорных механизмов, публичного регулирования и международных стандартов защиты прав. Владение цифровым активом означает не абсолютную автономию, а участие в сложной системе, где доступ к средствам зависит от совокупности технических и правовых факторов.

Mechanisms of Practice / Abuse / Ключевые механизмы практики, злоупотребления или конфликта

Первый ключевой механизм связан с технической возможностью централизованного замораживания токенов. Многие эмитенты стейблкоинов сохраняют административные функции, позволяющие блокировать определённые адреса, запрещать переводы и делать токены фактически непригодными к использованию. Для пользователя это означает, что даже при наличии приватных ключей контроль над активом может быть ограничен извне. Частная компания получает возможность мгновенно превратить цифровую ликвидность в неподвижную запись в блокчейне. На практике техническая архитектура многих стейблкоинов остаётся под воздействием централизованных правовых и комплаенс-механизмов.

Второй механизм заключается в применении санкционных режимов. Эмитенты, биржи и поставщики услуг обязаны учитывать ограничения, вводимые национальными и международными органами. Если адрес, пользователь или связанная с ними структура попадают под санкционные критерии либо интерпретируются как связанные с санкционным риском, операции могут быть немедленно остановлены, а активы заморожены.

Третий механизм связан с использованием аналитики блокчейна. Специализированные компании отслеживают происхождение токенов, движение средств между адресами и предполагаемые связи с высокорискованными кошельками, платформами или юрисдикциями. На основе таких данных формируются внутренние оценки риска. Даже косвенная связь с адресом, ранее использованным третьими лицами, может привести к ограничениям.

Четвёртый механизм состоит в договорных полномочиях эмитентов и платформ. Пользовательские соглашения обычно предоставляют компаниям широкую свободу ограничивать доступ, запрашивать дополнительные сведения, задерживать операции и прекращать обслуживание. Формально пользователь соглашается с этими условиями заранее, хотя практическое значение таких положений нередко недооценивается.

Пятый механизм связан с внутренними комплаенс-процедурами криптовалютных бирж и кастодиальных сервисов. Платформа может заблокировать вывод средств, запросить документы о происхождении активов, потребовать объяснения по отдельным транзакциям или закрыть учётную запись без окончательного судебного решения. При этом стандарты доказанности и процедуры пересмотра определяются самой компанией.

Шестой механизм заключается в исполнении судебных актов, регуляторных предписаний и запросов правоохранительных органов. Эмитенты и поставщики услуг могут реагировать не только на окончательные решения суда, но и на временные меры, запросы органов расследования и административные распоряжения.

Седьмой механизм связан с репутационным и контрагентским эффектом. Если адрес или пользователь получают статус повышенного риска, другие участники рынка могут отказываться принимать токены, ограничивать сотрудничество или требовать дополнительные проверки. В результате технически ликвидный актив становится экономически затруднительным в использовании.

Восьмой механизм состоит в сочетании традиционного банковского контроля и криптовалютного комплаенса. Пользователь может одновременно столкнуться с блокировкой банковских переводов, ограничением на бирже, замораживанием стейблкоинов и требованиями предоставить дополнительные документы. Формально каждое решение принимается отдельно, но фактически они образуют единую систему давления.

Девятый механизм связан с трансграничностью цифровых активов. Эмитент может находиться в одной юрисдикции, пользователь в другой, биржа в третьей, а активы и транзакции затрагивать множество государств одновременно. Это усложняет выбор применимого права, определение компетентного суда и выработку эффективной стратегии защиты.

Десятый механизм заключается в длительном сохранении негативного профиля. Даже после снятия ограничений информация о предыдущей блокировке или повышенном риске может оставаться во внутренних системах компаний и влиять на последующие решения. В результате формальное восстановление доступа не всегда означает полноценное восстановление доверия и функциональности актива.

Case Patterns / Типовые сценарии, модели развития ситуации или практика применения

Первый типовой сценарий связан с блокировкой стейблкоинов по требованию государственного органа или в рамках внутреннего решения эмитента. Пользователь обнаруживает, что токены по-прежнему отображаются в кошельке, но не могут быть переведены, обменены или использованы в расчётах. С технической точки зрения актив существует, однако экономически он становится недоступным. Для владельца это выглядит как цифровой аналог ареста имущества без традиционной процедуры физического изъятия.

Второй сценарий возникает при использовании криптовалютной биржи или кастодиального сервиса. Платформа может внезапно остановить вывод средств, запросить документы о происхождении активов, сведения о контрагентах, налоговые документы, судебные

материалы или объяснения по конкретным операциям. Пока проверка продолжается, пользователь фактически лишён доступа к ликвидности, а сроки рассмотрения нередко остаются неопределёнными.

Третий сценарий связан с ошибочной или чрезмерно широкой интерпретацией данных блокчейн-аналитики. Адрес может быть классифицирован как рискованный из-за косвенной связи с кошельком, который ранее участвовал в подозрительной транзакции. При этом владелец токенов не совершал противоправных действий и может даже не знать о происхождении части активов. Тем не менее ограничения применяются автоматически, поскольку внутренняя система воспринимает адрес как источник риска.

Четвёртый сценарий возникает в связи с санкционным регулированием. Пользователь может столкнуться с блокировкой активов не потому, что он включён в официальный санкционный список, а потому что его профиль, юрисдикция, деловые связи или отдельные операции интерпретируются как связанные с санкционным риском. Частные компании, стремясь минимизировать собственную ответственность, нередко применяют более жёсткие ограничения, чем это прямо требуется законом.

Пятый сценарий касается трансграничных споров и уголовных дел. Если лицо фигурирует в расследовании, экстрадиционном процессе, международном розыске или корпоративном конфликте, криптовалютные платформы и эмитенты могут рассматривать это как основание для усиленного контроля или ограничения доступа к активам. В результате цифровые активы, которые использовались как альтернатива банковской системе, оказываются включёнными в ту же комплаенс-инфраструктуру.

Шестой сценарий связан с утратой доступа к учётной записи. Даже если токены не заморожены непосредственно на уровне смарт-контракта, пользователь может потерять возможность распоряжаться ими из-за закрытия аккаунта, технической блокировки, отказа в прохождении повторной идентификации или невозможности предоставить документы в требуемой форме.

Седьмой сценарий возникает при наследовании, банкротстве, разделе имущества или исполнении судебных решений. Стейблкоины рассматриваются как имущественный актив, который может быть предметом взыскания, ареста, передачи наследникам или распределения между сторонами спора. Отсутствие чётких процедур и различия между юрисдикциями создают дополнительные правовые риски.

Восьмой сценарий связан с использованием стейблкоинов в странах с валютными ограничениями, банковской нестабильностью или ограниченным доступом к международным платежам. Для пользователей такие активы становятся критически важным инструментом сохранения стоимости. Их блокировка может привести к немедленной утрате доступа к средствам для проживания, оплаты лечения, юридической защиты и поддержки бизнеса.

Девятый сценарий касается последующего восстановления доступа. Даже после предоставления всех документов, снятия санкционных или процессуальных рисков и положительного решения компании пользователь может столкнуться с длительными задержками, частичным восстановлением функциональности или сохранением статуса повышенного риска. Формальное снятие ограничений не всегда возвращает активу прежнюю степень ликвидности и доверия.

Десятый сценарий представляет собой сочетание нескольких факторов одновременно: уголовного дела, санкционного риска, блокчейн-аналитики, банковских ограничений и действий частных платформ. В таких ситуациях владелец активов сталкивается не с

единичным техническим сбоем, а с комплексной системой взаимосвязанных ограничений, каждое из которых усиливает остальные. Именно такие случаи представляют наибольшую сложность для правовой защиты и требуют координированной международной стратегии.

Risk Assessment / Основные риски, правовые уязвимости и проблемные зоны

Первый риск заключается в ошибочном восприятии стейблкоинов как полностью автономного и неподконтрольного инструмента. Пользователь может полагать, что наличие приватных ключей гарантирует абсолютный контроль над активом. На практике централизованные эмитенты сохраняют техническую возможность замораживать токены, а биржи и кастодиальные сервисы способны ограничивать доступ к средствам. Юридическая реальность оказывается значительно менее романтичной, чем рекламные обещания о финансовой свободе.

Второй риск связан с концентрацией полномочий у частных компаний. Эмитенты стейблкоинов, криптовалютные платформы и аналитические сервисы принимают решения, способные фактически лишить человека доступа к активам на миллионы долларов. При этом процедуры пересмотра, раскрытие оснований и стандарты доказанности определяются самими компаниями и нередко существенно уступают судебным гарантиям.

Третий риск состоит в непрозрачности алгоритмической оценки. Блокчейн-аналитика использует сложные модели классификации адресов и транзакций, однако пользователь обычно не знает, какие именно данные были использованы, какие связи послужили основанием для подозрений и насколько достоверны выводы. Ошибка в такой системе может иметь немедленные и крайне дорогостоящие последствия.

Четвёртый риск связан с санкционным регулированием. Даже если лицо не включено в официальный санкционный список, его операции, деловые связи, гражданство, страна проживания или взаимодействие с определёнными адресами могут быть интерпретированы как повышенный риск. Частные компании часто действуют по принципу максимальной осторожности и предпочитают блокировать активы, чем вступать в спор с регуляторами.

Пятый риск заключается в смешении правовых и технических ограничений. Пользователь может не понимать, действует ли замораживание на уровне смарт-контракта, на уровне биржи, на основании судебного акта, санкционного требования или внутреннего решения службы комплаенса. Без точного определения источника ограничения невозможно выбрать эффективный механизм защиты.

Шестой риск связан с трансграничностью структуры. Эмитент, биржа, кастодиальный сервис, пользователь, банк и контрагенты могут находиться в разных юрисдикциях, каждая из которых применяет собственные правила. Это усложняет определение применимого права, компетентного суда, порядка вручения документов и перспектив исполнения решений.

Седьмой риск состоит в ограничении ликвидности в критический момент. Блокировка стейблкоинов может сделать невозможной оплату юридической защиты, исполнения контрактов, налогов, лечения, аренды и других обязательных расходов. Актив формально существует, но не выполняет свою экономическую функцию.

Восьмой риск связан с сохранением негативного комплаенс-профиля. Даже после разблокировки информация о предыдущих ограничениях может оставаться в системах эмитента, биржи или аналитической компании, влияя на будущие решения и повышая вероятность повторных ограничений.

Девятый риск заключается в недостаточной правовой определённости. Во многих юрисдикциях регулирование цифровых активов продолжает развиваться, а судебная практика остаётся ограниченной. Это создаёт неопределённость относительно объёма имущественных прав, допустимых ограничений и способов их защиты.

Десятый риск состоит в ложном ощущении диверсификации. Пользователь может считать, что уход из традиционной банковской системы устраняет юридические угрозы. На практике стейблкоины и связанные платформы встроены в столь же строгую, а иногда и более оперативную систему санкционного и комплаенс-контроля. То есть цифровой кошелёк не отменяет реальность, он просто меняет форму бюрократии.

Institutional Gaps / Институциональные ограничения, пробелы, дефицит гарантий или системные слабости

Первая системная слабость заключается в том, что технологическая инфраструктура цифровых активов развивается значительно быстрее, чем правовые механизмы защиты пользователей. Эмитенты стейблкоинов, криптовалютные биржи и поставщики кастодиальных услуг способны технически замораживать активы и ограничивать операции практически мгновенно, тогда как судебные процедуры, административные жалобы и международные механизмы защиты требуют времени. В результате доступ к средствам может быть утрачен за считаные минуты, а восстановление прав занимает недели, месяцы или даже годы.

Вторая слабость состоит в концентрации фактической власти у частных компаний. Эмитент стейблкоина или крупная криптовалютная платформа принимает решения, сопоставимые по последствиям с государственным арестом имущества, но действует в рамках собственных пользовательских соглашений и внутренних политик. Пользователь формально связан договором, однако реального влияния на содержание этих условий не имеет. Частная инфраструктура начинает выполнять квазигосударственные функции без полного набора публично-правовых гарантий.

Третья слабость связана с ограниченной прозрачностью оснований для блокировки. Пользователь часто не получает полного объяснения, какие именно обстоятельства послужили причиной ограничения: санкционный риск, данные блокчейн-аналитики, запрос правоохранительных органов, подозрение в нарушении правил платформы или совокупность нескольких факторов. Без понимания источника проблемы защита превращается в попытку спорить с чёрным ящиком, который сообщает лишь итоговый результат.

Четвёртая слабость заключается в зависимости рынка от небольшого числа крупных участников. Несколько эмитентов, аналитических компаний и глобальных платформ фактически формируют стандарты поведения для всей отрасли. Ошибочная классификация, техническая ошибка или чрезмерно осторожная политика одного ключевого участника могут повлиять на доступ пользователя к значительной части цифровой финансовой инфраструктуры.

Пятая слабость состоит в том, что алгоритмические оценки и внутренние комплаенс-модели не всегда подлежат независимой проверке. Пользователь не имеет доступа к методологии, исходным данным и внутренним правилам классификации риска. Даже если выводы являются ошибочными, опровергнуть их бывает крайне сложно, поскольку процесс принятия решения остаётся непрозрачным.

Шестая слабость связана с фрагментацией юрисдикций. Эмитент может быть зарегистрирован в одной стране, иметь операционные структуры в другой, хранить резервы в третьей,

использовать поставщиков аналитики в четвёртой, а обслуживать пользователя, находящегося в пятой. Такая структура усложняет определение применимого права, выбор компетентного суда и реальное исполнение решений.

Седьмая слабость заключается в отсутствии единообразных стандартов восстановления после ошибочной блокировки. Даже если пользователь предоставляет все требуемые документы и доказывает отсутствие нарушений, сроки рассмотрения, критерии пересмотра и порядок снятия ограничений часто остаются неопределёнными. В некоторых случаях решение принимается, но доступ к активам восстанавливается частично или с существенными задержками.

Восьмая слабость состоит в недостаточном учёте права собственности и процессуальных гарантий в частных решениях. Формально ограничения основаны на договоре и комплаенс-политике, однако фактически они затрагивают имущественные права, экономическую деятельность и способность человека пользоваться собственными средствами. Юридическая система ещё не выработала единообразный баланс между свободой договора и необходимостью защищать пользователей от непропорциональных ограничений.

Девятая слабость связана с долговечностью негативной информации. Сведения о прошлых блокировках, запросах дополнительных документов или подозрениях могут сохраняться в внутренних базах и аналитических системах даже после разрешения проблемы. Это создаёт риск повторных ограничений и затрудняет полное восстановление финансовой репутации.

Десятая слабость заключается в институциональной склонности к максимальной осторожности. Для компании проще заморозить активы, чем впоследствии объяснять регулятору, почему она не предприняла меры. Для аналитического сервиса безопаснее присвоить адресу повышенный уровень риска. Для платформы проще отказать в операции, чем разбираться в сложном фактическом контексте. Такая логика рациональна с точки зрения внутреннего контроля, но она переносит основную тяжесть неопределённости на владельца цифровых активов.

Practical Guidance / Практические рекомендации и модель правового действия

Первый практический шаг состоит в том, чтобы рассматривать стейблкоины не как «цифровые доллары в вакууме», а как активы, встроенные в сложную правовую и технологическую инфраструктуру. Перед использованием конкретного токена необходимо понимать, кто является его эмитентом, в какой юрисдикции он действует, какие полномочия по замораживанию закреплены в пользовательских документах, какие санкционные и комплаенс-правила применяются и какие механизмы рассмотрения споров доступны. Технология может выглядеть современной и изящной, но договор мелким шрифтом по-прежнему управляет значительной частью реальности.

Второй шаг заключается в диверсификации инфраструктурных рисков. Не следует концентрировать все средства на одной бирже, в одном кастодиальном сервисе или в одном типе актива. Целесообразно распределять ликвидность между различными кошельками, платформами и, при необходимости, несколькими формами хранения. Цель состоит не в том, чтобы избежать регулирования, а в том, чтобы снизить вероятность полной потери доступа в результате одного корпоративного или комплаенс-решения.

Третий шаг состоит в поддержании документальной готовности. Владельцу активов рекомендуется заранее хранить документы, подтверждающие происхождение средств, историю операций, договоры, налоговые декларации, корпоративные документы и иные материалы, которые могут потребоваться при проверке. Когда платформа внезапно

запрашивает объяснения, заранее подготовленные документы существенно повышают эффективность взаимодействия с платформой.

Четвёртый шаг связан с технической самостоятельностью. По возможности следует использовать некостодиальные кошельки и контролировать приватные ключи. Это не исключает риска замораживания на уровне эмитента, но уменьшает зависимость от решений биржи или кастодиального посредника. Если ключи находятся у третьего лица, ваши активы в значительной степени находятся там же, независимо от маркетинговых обещаний.

Пятый шаг заключается в постоянном мониторинге юрисдикционных и санкционных рисков. Владельцам активов необходимо отслеживать изменения в регулировании, новые санкционные меры, требования к раскрытию информации и изменения в политике платформ. Особенно важно учитывать риски, связанные со страной проживания, гражданством, деловыми партнёрами и характером операций.

Шестой шаг состоит в оперативной фиксации ограничений. При блокировке средств следует немедленно сохранять уведомления платформы, переписку, идентификаторы транзакций, скриншоты кошельков и иные доказательства. Эти материалы необходимы как для внутреннего пересмотра, так и для возможных судебных или административных действий.

Седьмой шаг связан с последовательной коммуникацией с эмитентом или платформой. Ответы должны быть структурированными, документированными и юридически выверенными. Следует ясно разделять подтверждённые факты, пояснения пользователя и правовые аргументы. Структурированные и документально подтверждённые обращения, как правило, являются наиболее эффективным способом взаимодействия с комплаенс-подразделениями.

Восьмой шаг заключается в определении источника ограничения. Необходимо установить, происходит ли блокировка на уровне смарт-контракта, биржи, кастодиального сервиса, санкционного требования, судебного решения или внутреннего алгоритма риска. От этого зависит выбор стратегии: договорный спор, судебное разбирательство, административное обращение или международная защита.

Девятый шаг состоит в подготовке трансграничной стратегии. Если активы, платформы и участники находятся в разных странах, необходимо заранее определить применимое право, потенциально компетентные суды, возможность получения обеспечительных мер и порядок исполнения решений. Без такого анализа защита рискует потеряться в географии быстрее, чем в самом споре.

Десятый шаг заключается в восстановлении финансовой и комплаенс-репутации после снятия ограничений. Даже после разблокировки средств рекомендуется направлять обновлённые документы, подтверждать изменение статуса, добиваться удаления устаревшей информации и фиксировать официальные подтверждения восстановления доступа. Формальное снятие блокировки не всегда означает, что система действительно забыла о вашем существовании.

Процессуальные гарантии при блокировке цифровых активов и использовании технических данных в качестве доказательств

В делах о стейблкоинах и иных цифровых активах ограничения доступа к средствам — блокировка адресов, замораживание балансов на платформе, приостановка вывода, отказ в исполнении транзакции, закрытие аккаунта — нередко применяются быстрее, чем любой судебный механизм. Это повышает значимость минимальных процессуальных гарантий, которые должны соблюдаться как государственными органами, так и частными провайдерами

(биржи, кастодианы, эмитенты, платёжные посредники), когда их решения фактически приводят к лишению лица контроля над активом.

Перечень не является универсальной моделью для всех юрисдикций; его задача — обозначить минимальные критерии добросовестности и проверяемости, критичные для прав человека, защиты собственности и справедливой процедуры. Гарантии должны применяться до наступления необратимых последствий, а не после.

Ниже приведён перечень ключевых гарантий, применимых при: (a) ограничении доступа к активам, (b) блокировке или замораживании средств, (c) использовании технических (ончейн / платформенных) данных в качестве доказательств.

1. Гарантии при принятии решения о блокировке или ограничении доступа к активам

1.1. Ясное правовое основание и идентификация инициатора меры

Должно быть понятно, что именно является основанием: санкционный режим, AML-подозрение, запрос органа, внутреннее правило платформы, риск-модель. Ключевой элемент — фиксация того, кто принял решение (орган, суд, компания) и в какой процедуре.

Проверяемые маркеры:

· указание на конкретный санкционный режим или норму AML-законодательства;
· идентификация органа или должностного лица, принявшего решение о блокировке;
· при блокировке на основании внутренней комплаенс-политики — ссылка на соответствующий пункт правил.

1.2. Уведомление лица и минимальная раскрываемость причин

Лицу должна быть предоставлена как минимум:

· категория основания (санкции / AML / мошенничество / похищенные средства / геориск и т.п.);
· перечень затронутых активов и операций;
· дата, время и объём ограничений;
· порядок и сроки оспаривания или пересмотра.

Допустимы исключения для предотвращения «tip-off» (предупреждения фигуранта), но они должны быть узкими и временными; иначе блокировка превращается в непрозрачное наказание. Если уведомление задержано на основании такого исключения, факт исключения и его основание должны быть задокументированы.

Проверяемые маркеры:

· наличие письменного уведомления (в электронной или иной форме);
· при задержке уведомления — документальное подтверждение основания для такой задержки.

1.3. Право быть выслушанным и представить документы

Необходим процедурный канал для представления объяснений и доказательств: source of funds / source of wealth, KYC-документы, контракты, подтверждение экономической цели, данные о

бенефициарном владении, доказательства добросовестности. Для санкционного комплаенса — также доказательства отсутствия совпадений, ошибочности матчей, различия идентификаторов.

Проверяемые маркеры:

· наличие доступного канала для подачи возражений и документов;
· разумный срок для представления объяснений;
· обязанность платформы или органа рассмотреть представленные материалы.

1.4. Мотивированность и индивидуализация меры (не только «risk score»)

Решение должно опираться не на общий «уровень риска», а на индивидуализированные обстоятельства: какие именно операции, адреса или контрагенты вызывают проблему и почему выбран именно такой объём ограничения.

Проверяемые маркеры:

· указание в решении на конкретные транзакции, адреса или периоды, вызвавшие подозрение;
· отсутствие ссылок только на абстрактную категорию риска без привязки к фактическим обстоятельствам.

1.5. Пропорциональность и наименее ограничительная альтернатива

Проверяется, возможно ли заменить полную блокировку:

· частичным лимитом;
· заморозкой только спорной суммы;
· разрешением операций для базовых нужд, налогов, оплаты защиты;
· переводом в режим повышенного мониторинга без лишения доступа.

В цифровых активах это критично: полная остановка часто равна экономической конфискации до разбирательства. При блокировке стейблкоина на уровне смарт-контракта следует оценивать, возможно ли заморозить только часть адресов, связанных с лицом, а не весь актив.

Проверяемые маркеры:

· документальное подтверждение, что менее строгие меры рассмотрены и признаны недостаточными;
· при блокировке всего счёта — объяснение, почему частичные ограничения не могли быть применены.

1.6. Сроки, пересмотр и автоматическое прекращение ограничения

Ограничение должно быть:

· ограничено по времени;
· подлежать регулярному пересмотру по мере поступления новых данных;
· прекращаться при исчезновении основания (обновление санкционных списков, снятие подозрения, подтверждение легитимности происхождения средств) — автоматически, без необходимости отдельного запроса со стороны пользователя.

Проверяемые маркеры:

· установленный срок действия ограничения (например, 30, 60 или 90 дней);
· процедура продления с обновлённым обоснованием;
· обязанность платформы или органа инициировать пересмотр при изменении обстоятельств.

1.7. Независимый механизм обжалования

Должна существовать возможность:

· внутреннего пересмотра (в компании — другим уровнем комплаенса или юристами);
· внешнего пересмотра (суд, арбитраж, омбудсмен, надзорный орган — в зависимости от модели).

Ключевой критерий — реальная способность изменить решение, а не формальная «кнопка апелляции».

Проверяемые маркеры:

· наличие письменной информации о порядке обжалования;
· разумный срок рассмотрения жалобы;
· документально зафиксированные случаи изменения решений по результатам обжалования.

2. Гарантии при использовании технических данных (ончейн-данных, логов платформы, блокчейн-аналитики) в качестве доказательств

2.1. Проверяемость происхождения данных и цепочки сохранности (chain of custody)

Должно быть документировано: кто собрал данные, когда, из каких источников, в каком виде они хранились и передавались, кто имел доступ, были ли изменения. Это одинаково важно для:

· ончейн-выгрузок;
· данных с биржи или кастодиана;
· IP/Device/геолокационных логов;
· отчётов блокчейн-аналитики.

Проверяемые маркеры:

· наличие временных меток и идентификаторов транзакций;
· документация о лицах, имевших доступ к данным;
· отсутствие признаков модификации или нарушения цепочки хранения.

2.2. Воспроизводимость метода и контроль ошибок

Если используются кластеризация адресов, attribution-метки, риск-скоринг, эвристики «travel rule», то должно быть понятно:

· какая методика применена;
· её пределы;
· вероятность ложных совпадений (включая ошибочную привязку адреса к подсанкционному лицу из-за использования общего кошелька биржи или миксера);

· какие допущения сделаны.

Вывод «адрес связан с X» без раскрытия метода должен рассматриваться как сигнал риска, а не как самодостаточное доказательство.

Проверяемые маркеры:

· указание на конкретное программное обеспечение или аналитический инструмент;
· описание методологии привязки адресов к лицам;
· раскрытие известных ограничений метода.

2.3. Разграничение «адрес / аккаунт» и «лицо»

Техническая связь транзакции с адресом не равна доказанности контроля конкретным лицом. Для вывода о владении или контроле должны оцениваться дополнительные признаки: ключи или подписи, данные кастодиана, устройства, поведенческие паттерны, документы KYC, контекст операций.

Проверяемые маркеры:

· наличие дополнительных доказательств, подтверждающих контроль лица над адресом;
· при отсутствии таких доказательств — признание вывода о контроле предположительным.

2.4. Контекст и экономический смысл операций

Технические данные должны интерпретироваться с учётом:

· роли смарт-контрактов, мостов, DEX, миксеров, batch-операций;
· специфики стейблкоинов (эмитент, контракты заморозки, blacklist-функции);
· различий между «получил токены» и «получил выгоду / контроль».

Без контекста высок риск ошибочной криминализации обычной инфраструктурной активности.

Проверяемые маркеры:

· учёт технических особенностей блокчейна при интерпретации данных;
· наличие в решении или отчёте анализа альтернативных объяснений (например, получение токенов в результате работы ликвидного пула, а не в качестве дохода).

2.5. Доступ защиты к данным и возможность контрэкспертизы

Сторона, чьи права ограничиваются, должна иметь возможность получить минимум данных, достаточный для проверки выводов и подготовки контрзаключения (в том числе независимой технической экспертизы), с соблюдением разумных ограничений конфиденциальности.

Проверяемые маркеры:

· предоставление стороне доступа к исходным данным (хеши, адреса, временные метки);
· при отказе в предоставлении — мотивированное объяснение причин;
· возможность привлечения независимого эксперта за счёт стороны или (в судебном порядке) за счёт средств правосудия.

---

3. Особые гарантии для стейблкоинов и провайдеров с административным контролем (эмитент / кастодиан)

3.1. Транспарентность роли эмитента или платформы

Если эмитент стейблкоина или кастодиан технически способен замораживать актив (freeze / blacklist), требуется ясность: мера принята по закону, по запросу органа, по внутренней политике компании; какие критерии применялись, какие сроки установлены, какие процедуры пересмотра предусмотрены. При блокировке, опосредованной смарт-контрактами и оракулами, должна быть ясна ответственность за принятие решения.

Проверяемые маркеры:

· раскрытие условий, при которых эмитент применяет функцию заморозки;
· указание на то, действует ли эмитент по собственной инициативе или во исполнение запроса государственного органа.

3.2. Разделение санкционного контроля и AML-подозрения

Санкции — это режим юридических запретов (часто формально-списочный). AML-подозрение — это риск-оценка. Смешение режимов ведёт к «санкционному эффекту без санкций»: бессрочным блокировкам на основании нераскрытого risk score.

Проверяемые маркеры:

· чёткое указание в решении, на каком правовом основании применена блокировка;
· если блокировка основана на AML-подозрении, а не на санкциях — указание на это и установление разумных сроков для проверки.

3.3. Защита добросовестных третьих лиц

Заморозка на уровне смарт-контракта или адреса может затронуть контрагентов и конечных получателей, не связанных с риском. Процедура должна учитывать права третьих лиц и предусматривать механизм выделения или разблокировки неоспариваемых сумм.

Проверяемые маркеры:

· наличие процедуры для третьих лиц, чьи активы затронуты блокировкой, по представлению доказательств своей добросовестности;
· возможность разблокировки части активов, не связанных с предполагаемым нарушением.

Минимальный стандарт добросовестной процедуры

Изложенные выше гарантии могут показаться технически детализированными. Однако в практике цифровых активов именно их отсутствие или систематическое игнорирование превращает блокировку из меры управления риском в инструмент непропорционального воздействия.

Минимальный стандарт добросовестной процедуры при ограничении доступа к цифровым активам включает: уведомление (в допустимом объёме) → мотивированность и индивидуализацию → право представить объяснения → пропорциональность и временные рамки → независимый пересмотр. При использовании технических данных дополнительно требуются: цепочка сохранности, воспроизводимость метода, разграничение «адрес / лицо», контекст операций и возможность контрэкспертизы.

Эти элементы критичны, потому что в цифровой среде блокировка часто наступает мгновенно, а последствия (финансовая изоляция, утрата ликвидности, прекращение обслуживания) могут быть необратимыми ещё до проверки по существу.

Policy Recommendations / Рекомендации по правовому и институциональному подходу

Во-первых, эмитенты стейблкоинов и поставщики услуг в сфере цифровых активов должны обеспечивать более прозрачные процедуры блокировки и разблокировки активов. Пользователь должен получать понятное уведомление о характере ограничения, разумный объём информации о его основании и реальную возможность представить документы и добиться пересмотра решения. Коммерческая конфиденциальность не должна превращаться в универсальный ответ на любой вопрос о судьбе чужих средств.

Во-вторых, необходимо развивать единые минимальные стандарты процессуальной справедливости для частных платформ. Если решение компании фактически ограничивает право собственности и доступ к ликвидности, пользователю должны быть доступны разумные сроки рассмотрения, мотивированный ответ и предсказуемая процедура обжалования.

В-третьих, регуляторы должны учитывать риск чрезмерной зависимости отрасли от небольшого числа централизованных участников. Концентрация полномочий по замораживанию активов и оценке риска в руках ограниченного круга компаний создаёт системную уязвимость и повышает вероятность непропорциональных последствий при ошибках или чрезмерно осторожных подходах.

В-четвёртых, санкционные и комплаенс-механизмы должны применяться на основе индивидуальной и актуальной оценки. Косвенные связи, технические совпадения и устаревшие сведения не должны автоматически приводить к бессрочному ограничению доступа к активам без дополнительной проверки.

В-пятых, регулирование цифровых активов должно прямо признавать, что стейблкоины и иные токены являются объектом имущественных прав. Соответственно, ограничения в отношении таких активов должны соответствовать принципам законности, необходимости, процессуальной справедливости и соразмерности.

В-шестых, международные стандарты в области противодействия легализации преступных доходов и санкционного контроля должны учитывать риск ошибочной классификации и предусматривать эффективные механизмы исправления последствий. Система, которая умеет только блокировать, но не умеет разумно восстанавливать доступ, напоминает дверь с одним режимом работы.

В-седьмых, регуляторы и отраслевые организации должны поощрять независимую проверяемость аналитических моделей. Пользователи не обязаны получать полный доступ к коммерческим алгоритмам, однако должны существовать процедуры, позволяющие оспаривать явно ошибочные выводы и предоставлять контрдоказательства.

В-восьмых, необходимо развивать трансграничные механизмы сотрудничества по вопросам восстановления доступа к цифровым активам. Когда пользователь, эмитент, платформа и активы находятся в разных странах, отсутствие координации существенно усложняет защиту права собственности.

В-девятых, правоприменительная практика должна рассматривать блокировку цифровых активов не как исключительно техническое действие, а как юридически значимое вмешательство в имущественные права. Это требует более строгого анализа необходимости и соразмерности, особенно когда ограничения затрагивают средства для проживания, лечения, юридической защиты или функционирования бизнеса.

В-десятых, владельцы цифровых активов должны восприниматься не только как участники технологической среды, но и как субъекты, обладающие полноценными имущественными и процессуальными правами. Эффективное регулирование должно одновременно обеспечивать борьбу с незаконным использованием цифровых активов и предотвращать непропорциональные ограничения в отношении добросовестных пользователей.

Conclusion / Заключение

Стейблкоины стали одним из ключевых инструментов современной цифровой экономики, объединив технологическую скорость, глобальную ликвидность и относительную ценовую стабильность. Для миллионов пользователей они представляют собой удобное средство хранения стоимости, расчётов и доступа к трансграничной финансовой инфраструктуре.

Однако практическое использование стейблкоинов показывает, что цифровой актив не существует вне правового контекста. Возможность эмитента замораживать токены, решения бирж и кастодиальных платформ, санкционные режимы, аналитика блокчейна и внутренние комплаенс-процедуры формируют систему, в которой доступ к средствам зависит не только от технологии, но и от множества юридических и институциональных факторов.

Главный вывод настоящего доклада состоит в том, что стейблкоины следует рассматривать как регулируемые имущественные активы, а не как полностью автономную форму капитала. Их использование требует такого же внимательного отношения к юрисдикции, договорным условиям, санкционным рискам, происхождению средств и структуре хранения, какого требует работа с традиционной финансовой системой. Иными словами, блокчейн не отменил юридическую реальность, а лишь придал ей более футуристический интерфейс.

Для ARGA данная тема имеет особое значение, поскольку цифровые активы всё чаще становятся частью международных споров, корпоративных конфликтов, процедур защиты собственности и стратегий финансовой мобильности. Эффективная правовая защита в этой области должна объединять знания в сфере регулирования цифровых активов, санкционного права, финансового мониторинга, международной юрисдикции, договорного права и защиты прав человека.

Только комплексный подход позволяет обеспечить разумный баланс между необходимостью предотвращать незаконное использование цифровых активов и обязанностью защищать добросовестных владельцев от ошибочных, непрозрачных и несоразмерных ограничений. В конечном счёте вопрос заключается не только в технологии, но и в старом добром юридическом принципе: собственность должна быть защищена, даже если она записана не на бумаге, а в распределённом реестре.

Приложение А. Терминология

Стейблкоин. Цифровой актив, предназначенный для поддержания относительно стабильной стоимости за счёт привязки к фиатной валюте, корзине активов или иным резервным механизмам.

Цифровой актив. Имущественное право или цифровой объект стоимости, существующий в форме записи в распределённом реестре или иной аналогичной системе.

Эмитент. Юридическое лицо, осуществляющее выпуск, погашение и администрирование стейблкоина или иного централизованно управляемого цифрового актива.

Кастодиальный сервис. Организация, которая хранит приватные ключи или иным образом контролирует доступ пользователя к цифровым активам.

Некастодиальный кошелёк. Программное или аппаратное средство, в котором пользователь самостоятельно контролирует приватные ключи и распоряжается цифровыми активами без участия посредника.

Аналитика блокчейна. Технический анализ данных распределённого реестра, используемый для отслеживания транзакций, выявления связей между адресами и присвоения показателей риска.

Санкционный комплаенс. Совокупность процедур, направленных на соблюдение ограничительных мер и предотвращение операций, нарушающих санкционное законодательство.

Замораживание активов. Ограничение, исключающее возможность перевода, обмена, погашения или иного использования цифровых либо традиционных активов.

Риск-ориентированный подход. Методология, при которой интенсивность проверки и объём ограничений зависят от предполагаемого уровня правового, санкционного и комплаенс-риска.

Процессуальная справедливость. Минимальные гарантии, позволяющие лицу понять основания ограничения, представить документы и добиться содержательного пересмотра решения.

Право собственности. Юридически защищённое право владеть, контролировать, использовать и распоряжаться активами.

Международный контур ограничений. Совокупность трансграничных правовых, технических и комплаенс-последствий, влияющих на доступ к активам.

Приложение В. Матрица рисков / полномочий / правовых последствий

Действие	**Правовой риск**	**Юридический предел**	**Возможные последствия**	**Практический комментарий**
Замораживание токенов эмитентом	Утрата фактического контроля над активами	Ограничение должно основываться на договорных полномочиях и применимом праве	Невозможность перевода, обмена или погашения стейблкоинов	Необходимо установить, действует ли блокировка на уровне смарт-контракта или платформы

Ограничение учётной записи на бирже	Потеря доступа к ликвидности	Действия должны соответствовать договорным условиям и обязательным нормам защиты пользователей	Блокировка вывода средств и длительная проверка	Следует направлять структурированные и документально подтверждённые объяснения
Совпадение с санкционными критериями	Квалификация как санкционного риска	Ограничения должны основываться на индивидуальной и актуальной оценке	Блокировка операций и замораживание активов	Необходимо анализировать как прямые, так и косвенные связи с санкционными факторами
Негативная оценка аналитики блокчейна	Ошибочная классификация адреса	Выводы аналитических систем могут быть неполными или неточными	Усиленная проверка и ограничения операций	Следует добиваться пересмотра и представлять контрдоказательства
Прекращение кастодиального обслуживания	Потеря оперативного доступа к активам	Должны учитываться подтверждённые права пользователя и актуальные документы	Закрытие учётной записи и нарушение текущих операций	Рекомендуется использовать диверсифицированную систему хранения
Судебное или регулятор ное предписание	Формальное ограничение права распоряжения активами	Меры должны отвечать требованиям законности и соразмерности	Арест, замораживание или ограничения на использование средств	Необходимо получить и проанализировать правовое основание
Конфликт юрисдикций	Неопределённость применимого права и компетентного суда	Полномочия разных государств могут пересекаться	Задержки, рост расходов и сложность исполнения решений	Следует заранее готовить координированную международную стратегию
Сохранение негативного комплаенс-профиля	Продолжение квалификации как источника повышенного риска	Историческая информация должна обновляться после изменения обстоятельств	Повторные ограничения и репутационные потери	Необходимо добиваться официального подтверждения восстановления статуса

Официальные источники

Группа разработки финансовых мер борьбы с отмыванием денег (FATF), Руководство по риск-ориентированному подходу к виртуальным активам и поставщикам услуг, связанным с виртуальными активами.

Регламент (ЕС) 2023/1114 о рынках криптоактивов (MiCA).

Регламент (ЕС) 2023/1113 об информации, сопровождающей переводы денежных средств и отдельных криптоактивов.

Нормативные акты и разъяснения Управления по контролю за иностранными активами Министерства финансов США (OFAC).

Регламенты Европейского союза о санкциях и ограничительных мерах.

Европейская конвенция о защите прав человека и основных свобод.

Практика Европейского суда по правам человека по вопросам защиты права собственности.

Материалы Организации Объединённых Наций по вопросам цифровых финансов и незаконных финансовых потоков.

Публикации Банка международных расчётов по вопросам стейблкоинов и цифровых активов.

Доклады Совета по финансовой стабильности о глобальных механизмах обращения стейблкоинов.

Материалы Базельского комитета и Basel Institute on Governance по вопросам криптоактивов, комплаенса и финансовой добросовестности.

Financial Action Task Force, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA).

Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets.

United States sanctions regulations and guidance issued by the Office of Foreign Assets Control.

European Union restrictive measures and sanctions regulations.

European Convention on Human Rights.

Case law of the European Court of Human Rights concerning property rights.

United Nations materials on digital finance and illicit financial flows.

Bank for International Settlements publications on stablecoins and digital assets.

Financial Stability Board reports on global stablecoin arrangements.

Basel Committee and Basel Institute on Governance materials on crypto-assets, compliance and financial integrity.